epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

June 19, 2018

The Honorable Richard Burr, Chair
The Honorable Mark Warner, Ranking Member
U.S. Senate Select Committee on Intelligence
211 Hart Senate Office Building
Washington, DC 20510

Dear Chairman Burr and Ranking Member Warner:

We write to you regarding your open hearing on "Policy Response to Russian Interference in the 2016 U. S. Elections"[1] and the FBI's failure to notify hundreds of government officials that Russian actors compromised their email. The Electronic Privacy Information Center ("EPIC") is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[2]

After reports emerged about Russian interference with the 2016 election, EPIC launched a new project on Democracy and Cybersecurity.[3] EPIC is pursuing several Freedom of Information Act cases to learn more about the Russian interference in the 2016 Presidential election.[4] The Committee should be interested in the documents EPIC obtained in one of our FOIA cases, *EPIC v. FBI*,[5] concerning victim notification procedures, particularly after the subsequent report from the Associated Press that detailed the failure of the FBI to notify US targets of a foreign cyber attack.[6]

In *EPIC v. FBI*, EPIC we sought to understand and assess the FBI's response to the Russian interference in the 2016 Presidential election. As PPD-41 sets out, the FBI is the lead federal agency for investigating cyber attacks in the United States by criminals, overseas adversaries, and terrorists."[7] But questions were raised about the failure of the FBI to adequately investigate the

---

[1] *Policy Response to Russian Interference in the 2016 U. S. Elections*, 115th Cong. (2018), S. Select Comm. on Intelligence, https://www.intelligence.senate.gov/hearings/open-hearing-policy-response-russian-interference-2016-u-s-elections (June 20, 2018).
[2] *See* EPIC, *About EPIC*, https://epic.org/epic/about.html.
[3] *See* EPIC, *Democracy and Cybersecurity*, https://epic.org/democracy/.
[4] *EPIC v. ODNI*, No. 17-163 (D.D.C. filed Jan. 25, 2017); *EPIC Seeks Release of FISA Order for Trump Tower*, EPIC (March 6, 2017), https://epic.org/2017/03/epic-seeks-release-of-fisa-ord.html; *EPIC v. IRS*, No. 17-670 (D.D.C. filed Apr. 15, 2017).
[5] *EPIC v. FBI*, 2018 U.S. Dist. LEXIS 85467 *; 2018 WL 2324084 (D.D.C. May 22, 2018); EPIC v. FBI (Russian Hacking), https://epic.org/foia/fbi/russian-hacking/.
[6] Jeff Donn, Desmond Butler, Raphael Satter, *FBI deviated from its policy on alerting hacking victims,* San Francisco Chronicle (Nov. 27, 2017), http://www.sfchronicle.com/business/technology/article/FBI-deviated-from-its-policy-on-alerting-hacking-12387471.php
[7] *What We Investigate, Cyber Crime*, FBI.gov, https://www.fbi.gov/investigate/cyber; Directive on United States Cyber Incident Coordination ("PPD 41"), 2016 Daily Comp. Pres. Doc. 495 (July 26, 2016) (setting

attacks on the nation's political institutions.[8] EPIC therefore pursued records in the possession of the FBI to help the "public. . . . evaluate the FBI response to the Russian interference, assess threats to American democratic institutions, and to ensure the accountability of the federal agency with the legal authority to safeguard the American people against foreign cyber attacks."[9]

EPIC requested four sets of documents from the FBI:

(1) All records including, but not limited to, memos, reports, guidelines, procedures, summaries, and emails pertaining to the FBI's investigation of Russian-sponsored cyber attack on the RNC, DNC, and DCCC.
(2) All records of communications to the RNC, DNC, and DCCC regarding the threat of Russian interference in the 2016 Presidential election.
(3) All records of communications with other federal agencies regarding Russian interference in the 2016 Presidential election.
(4) All records including, but not limited to, memos, reports, guidelines, and procedures pertaining to the FBI's procedure to notify targets of cyber attacks.

As a result of the FOIA lawsuit, EPIC has obtained document set (4) regarding FBI procedures for notifying victims of cyberattacks. According to the FBI procedure for "Victim Notification in Computer Intrusion Matters" in the Cyber Division (CyD) Policy Guide (emphasis added) set out in the documents EPIC received:

> CyD's top priority is the protection of our national security, economy, and information infrastructure from intrusions, malicious code, and nefarious computer network operations. This effort entails the sharing of investigative information with intrusion victims and the CND community to protect compromised systems, mitigate economic loss and damage, and prevent future attacks. Victim notification is a compelling way for CyD to contribute to network defense for the protection of individual, commercial, and government users of the Internet, as well as for the protection of the infrastructure itself. It is the policy of CyD to notify and disseminate meaningful information to victims and the CND community in a timely manner to the extent to which it does not interfere with ongoing law enforcement or USIC investigations, operations, methods, sources, or technologies.
>
> In a computer intrusion investigation, the victim to be notified is the individual, organization, or corporation that is the owner or operator of the computer at the point of compromise or intrusion. Cyber victims are generally individuals or organizations subjected to cyber-based operations, including computer network attack (CNA) and computer network exploitation (CNE), in furtherance of criminal activity or threats to national security. These CNA and CNE operations often result in the compromise of

---

forth the FBI's legal authority for cybersecurity threat response).

[8] Ellen Nakashima & Adam Entous, *FBI and CIA Give Differing Accounts to Lawmakers on Russia's Motives in 2016 Hacks*, Wash. Post (Dec. 10, 2016), https://www.washingtonpost.com/world/national-security/fbi-and-cia-give-differing-accounts-to- lawmakers-on-russias-motives-in-2016-hacks/2016/12/10/c6dfadfa-bef0-11e6-94ac- 3d324840106c_story.html.

[9] Complaint at 7, *EPIC v. FBI*, *supra* note 5.

> electronic systems, resulting in the alteration, loss, exfiltration, or denial of access to data that the victim maintains or controls. Victims may be identified, to the extent possible, by the FBI or its partner agencies in the course of investigative activities of suspected cybercrimes and cyber-related threats.
>
> Because timely victim notification has the potential to completely mitigate ongoing and future intrusions and can mitigate the damage of past attacks while increasing the potential for the collection of actionable intelligence, CyD's policy regarding victim notification is designed to strongly favor victim notification. Even when it may interfere with another investigation or USIC operation, notification should still be considered in coordination with the operational stakeholders when the equities of victim notification serve to protect USPERs, a national infrastructure, or other U.S. interests from significant harm.[10]

The District Court in *EPIC v. FBI* acknowledged the significance of this inquiry. As the Court stated:

> As EPIC stresses, Russian interference in the 2016 presidential election is an important matter which has undoubtedly captured the attention of the American people and their elected representatives. Congress has made the issue a priority. The Senate Intelligence Committee is conducting a bipartisan investigation, armed with the power to compel testimony and documents, and reporting the information that it believes the public needs. The United States intelligence community is also actively investigating and has issued public reports, as EPIC notes. Special Counsel Mueller is leading a team of investigators and attorneys to explore Russian interference and to hold wrongdoers accountable.[11]

However, the Court, somewhat surprisingly, sided with the FBI on its claims that it need not release further information to EPIC.

> In this context, EPIC's purported goals of enabling "the public to evaluate the FBI response to the Russian interference, assess threats to American democratic institutions, and to ensure the accountability of the [FBI]," are best served by allowing federal investigators and lawmakers to conduct their missions on their timetables without the forced piecemeal dissemination of internal government documents relating to these ongoing efforts.[12]

So, this hearing before the House Judiciary Committee and House Oversight Committee provides a critical opportunity to "evaluate the FBI response to the Russian interference, assess threats to American democratic institutions, and to ensure the accountability of the [FBI]."As you aware, the Intelligence community assessed that both the DNC and the RNC were subject to a cyber

[10] Cyber Division Policy Guide at 4.7, *available at* https://epic.org/foia/fbi/russian-hacking/EPIC-16-12-22-FBI-FOIA-20170511-Production-2.pdf.
[11] *EPIC v. FBI*, 2018 U.S. Dist. LEXIS 85467, *16. (citations to the record omitted).
[12] *Id.*

attack by the Russian government.[13] And now we know that the FBI did not follow the required procedures for Victim Notification once the Bureau learned of this attack.

Based on the documents already obtained in *EPIC v. FBI* and the related reporting by the Associated Press, we request that the Committee ask the FBI:

- Will the FBI comply with government transparency laws and inform the public of the details of Russia's attempts to influence the outcome of a U.S. presidential election?
- How many cyberattack victims have not been notified that their email may have been compromised due to the FBI's failure follow the procedures set forth in the "Victim Notification in Computer Intrusion Matters" Policy Guide?
- Does the Policy Guide establish adequate procedures for cyber attacks on US political organizations or should new policies be adopted?
- Did the FBI do all it should have done to alert the DNC and the RNC once it learned about cyber attacks?
- Will the FBI follow the procedures set forth in the "Victim Notification in Computer Intrusion Matters" Policy Guide for the 2018 elections?

It is stunning that the FBI failed to follow its own written procedures, particularly where the cyber attack may have threatened national security. And it is vitally important that the American public is fully informed about the extent of Russian interference with the 2016 election.[14]

EPIC will keep you apprised of the documents we receive in our FOIA cases. We look forward to working with the Committee on the cybersecurity risks to democratic institutions.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Caitriona Fitzgerald*
Caitriona Fitzgerald
EPIC Policy Director

/s/ *Christine Bannan*
Christine Bannan
EPIC Policy Fellow

Attachment

FBI Cyber Division Policy Guide (CyD), "Victim Notification in Computer Intrusion Matters" (Obtained in EPIC v. FBI, No. 17-121 (D.D.C. filed Jan. 18, 2017).

[13] Office of the Dir. of Nat'l Intelligence, *Assessing Russian Activities and Intentions in Recent US Elections* (2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf [hereinafter Declassified ODNI Assessment].
[14] Marc Rotenberg, *Americans have a right to know what intel community knows on Russia,* The Hill (Mar. 27, 2017), http://thehill.com/blogs/pundits-blog/the-administration/325862-americans-have-a-right-to-know-what-intel-community